# *FDM Filer "Security" Assurance Q/A*

***FDM"s Privacy Act Notice:*** Title I of the Ethics in Government Act of 1978, as amended (the Act), 5 U.S.C. app. § 101 et seq., and 5 C.F.R. Part 2634 of the Office of Government Ethics regulations require the reporting of this information. The primary use of the information on this report is for review by Government officials to determine compliance with applicable Federal laws and regulations. This report may also be disclosed upon request to any requesting person pursuant to section 105 of the Act or as otherwise authorized by law. Filers may inspect applications for public access of their own form upon request. Additional disclosures of the information on the report may be made: (1) to a Federal, State, or local law enforcement agency if the disclosing agency becomes aware of a violation or potential violation of law or regulation; (2) to a court or party in a court or Federal administrative proceeding if the Government is a party or in order to comply with a judge-issued subpoena; (3) to a source when necessary to obtain information relevant to a conflict of interest investigation or decision; (4) to the National Archives and Records Administration or the General Services Administration in records management inspections; (5) to the Office of Management and Budget (OMB) during legislative coordination on private relief legislation; and (6) in response to a request for discovery or for the appearance of a witness in a pending judicial or administrative proceeding, if the information is relevant to the subject matter.

## *What assurance do filer's have that their information can't be intercepted over the Internet? (Communication security)*

- FDM is a secure, web-based application. All communications between the FDM servers and the user's desktop/laptop computers use a 128 bit, DES approved HTTPS protocol – making it virtually impossible for someone to "snoop" on the communications. This is the same encryption and protocol that is used routinely, on a daily basis, to conduct business on the Internet. For example, almost all credit card transactions on the Internet use the same approach and protocol.

## *What assurance do filer's have that FDM's servers are protected from hackers? (Logical intrusion -- Hacker security)*

- FDM is hosted on a Microsoft Windows 2000 Server that has been hardened using the DISA Window 2000 Security Technical Implementation Guidance (STIG). Unneeded ports and services have been removed from the operating system. Servers are patched on a regular basis as Microsoft issues patches or guidance. Hardware firewalls and Intrusion Detection Systems (IDS) are monitoring and blocking unauthorized connections outside the enclave. The servers use Symantec antivirus software to check for viruses in real time and check all files weekly. Virus definitions are set to automatically download nightly. Logs are checked for unauthorized access or server problems on a weekly basis.

### *What assurance do filer's have that FDM's servers are protected from physical intrusion? (Physical security)*

- The servers are located in a secured server room located in the US Army Legal Services Agency space near Ballston Metro stop. This building has guards located at the entrance during the day and the building requires a security FOB to access the floor after hours. There is a cipher lock on the entrance door to the suite and an additional cipher lock on the server room door. The cipher locks have different combinations and only the system administrators and GSA building manager have the cipher codes to the server room door.

- The server room is climate controlled with both air conditioning and humidifiers to control heat and static electricity. Data backups are performed nightly and stored on a server in another Government facility at a different location. Security for that server and for the server room is comparable to the primary server location. Both server rooms are climate controlled with both air conditioning and humidifiers to control heat and static electricity.

### *Who can access a filer's report? (Information privacy)*

- The filer and any assistant the filer approves.
- The filer's SLC and the ethics counselor(s) that support that SLC.
- The filer's supervisor.
- The supervisor's SLC and the ethics counselor(s) that support that SLC.
- The ADAEO and any ethics counselor(s) that support the ADAEO.

### *Who can create/modify filer data in a report? (Information integrity)*

- The filer's ***assistant*** can ***create/modify*** filer data before the filer submits a report into the review process – once submitted, an assistant can only view the filer's data..
- A filer can ***create or modify*** filer data any time before it has been submitted for final ADAEO review – once submitted for that final review, a filer can only view his/her data.
- Reviewers can ***never*** create or modify filer data in a report.
- Reviewer's can ***add*** comments to a report. Further, comments entered by a reviewer cannot be modified or deleted by another reviewer. (Detail: The ADAEO can prevent a comment from showing in the SF278 of record.)

### *Who can print signed reports? (Paper copy integrity)*

- FDM can print four different versions of the SF-278, each "distinguished" by watermarks or other features to ensure proper use of paper copies in the business process. For example, FDM places a *DRAFT* watermark on any version of the SF278 that is printed before it is submitted into the review process. Similarly, once a report is submitted for review, FDM places a WORKING COPY

watermark on all printed versions of the SF-278 EXCEPT as outlined in the next two bullets.

- FDM enables only the ADAEO to print the “official” report for release in response to public request. This version is distinguished by lacking any watermark and having four digital signatures on it. (Detail: three signatures for termination filers).
- In the rare case when it is needed, FDM enables only the filer to print the version of the report used in the “paper process”. The filer is expected to ink-sign this document and pass it on for review. It is distinguished by the presence of ink-signatures of all of the reviewers.

- In all cases where FDM prints a version of a digitally signed report, signature blocks are automatically filled in with “digitally signed by” naming the signer and the date signed. Finally, in the (rare) case where a filer has opted to file via the paper process, his/her signature block is automatically filled in with a “signature on record” notation – indicating the need to attach the “ink-signed” version to complete the official record.


# *Security*

- DA Authority to Operate approved 2 Feb 05 - meets DoD Information Technology Security (ITSEC) Certification and Accreditation Process (DITSCAP).
- Some highlights:
  - Application access limited; pre-approval by OTJAG SOCO
  - Need AKO account or CAC card to log in.
  - All information access carefully controlled through “role management”
  - Only accepts digital signatures that are DOD PKI compliant. Checks that the signer is the person expected to sign. SecureXML server is JITC certified.
  - All information stored in access controlled SQL database on physically secured servers. SSN’s are stored encrypted as is the database access login/password.
  - All communication between user’s PC and FDM is 128 bit encrypted. (HTTPS).
  - Compliance with the DISA security guidelines and controls, NIPRNET security and connectivity guidelines, Internet protocol packet filtering, user identification and authentication, network and physical security protection for the system, policies, and SOPs.